Anno 3 – N. 56
29 Luglio 2004 - 26 Agosto 2004

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Particolari al caldo

Durante un temporale d'estate si diventa intimisti. È quasi mezzanotte e la tivù brilla dall'altra parte della stanza, a volume zero. Lo schermo lampeggia in sincronia con i cambi di sequenza di un film che vorrebbe essere comico. Le altre luci che brillano nell'oscurità sono quelle della base wireless e del router ADSL, oltre naturalmente a questi bit che diventano lettere appena sopra le mie dita.

Quando piove, al buio e al caldo, mentre scrivi, finisci per guardarti l'ombelico. Vedi le cose intorno a te e capisci che c'è in corso un inganno fondamentale. Se non ce ne accorgiamo noi, non se ne accorgerà veramente nessuno.

L'inganno è questo. Ci sono tante cose che non vanno. Decreto Urbani, tanto per farla facile? Azioni della Finanza? Se il grafico si comporta bene, nella pagina a destra si vede l'immagine di quello che una volta era un sito. O la brevettabilità del software? Fosse solo questo. Microsoft ha appena brevettato il corpo umano in quanto conduttore di segnali elettrici che possono trasportare dati. Non credo che il brevetto durerà molto, forse basteranno i parenti di qualche poveraccio che è morto folgorato dai cavi dell'alta tensione. Buffer overflow, lo chiamerebbe Microsoft. Peccato che nessuno lo potrà riavviare. E che non ci sia niente di buffer.

L'inganno, dicevo. Sacrosanto indignarsi per tutte queste cose. A patto di essere consapevoli che passano sopra la nostra testa. Firmiamo pure le petizioni online, ma coscienti che non servono a un k4$$0. E sia ben chiaro a tutti che pure il blocco del sito del Ministero dei beni culturali (come ha proposto un deputato dei verdi), non cambierà il decreto di una virgola. Scriviamo incazzati sui forum e sulle home page, consci che sono parole, e solo quello.

Tutto inutile, allora? No. Possiamo fare veramente qualcosa. Possiamo davvero incidere. A patto che sia concreta, locale, nella nostra realtà. Protestare contro i brevetti e non aprire una sezione di software libero sul nostro sito è un grave errore. Boicottare Urbani e lasciare che i nostri amici non-hacker pensino a Bill Gates come a un benefattore dell'umanità è pessima strategia. Indignarsi per la chiusura dei circuiti p2p0 e tenere a zero la nostra condivisione è ipocrita.

Lottiamo, sì. Su cose concrete, immediate, pratiche, di cui vediamo l'effetto. Cambiamo davvero le cose accanto a noi e non pensiamo soltanto a quelle lontane, troppo difficili da cambiare.

Le grandi lotte epocali le vuole qualcun altro, vuole che facciamo massa ai suoi ordini. Le rivoluzioni mondiali sono una truffa. Stiamoci attenti, sì; ma intanto lavoriamo concretamente intorno a noi. Possiamo cambiare il mondo se iniziamo dalla piastrella accanto a quella dove stiamo. Se puntiamo direttamente a Redmond, vicinanze di Seattle, o a Palazzo Chigi, Roma, facciamo solo un gran fumo, o delle grandi cazzate. Lottiamo, sì. con l'ombelico. Per cose concrete, da cambiare subito, oggi, domani mattina. Cose vere.

Oppure rilassiamoci sotto l'ombrellone, pronti a tornare più carichi e incazzati che mai. Anche questa potrebbe essere una strategia. E il temporale si sta allontanando...

theguilty@hackerjournal.it

Boss: TheGuilty@hackerjournal.it

I Ragazzi della redazione europea:
Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron S. de Pecher, Contents by MDR

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Direttore Responsabile: Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: **NEWBIE** (per chi comincia), **MIDHACKING** (per chi c'è già dentro) e **HARDHACKING** (per chi mangia pane e worm).

Per esempio, 432 esempi

Ho trovato un sito molto interessante che illustra degli esempi di tutti i linguaggi di programmazione; lo si può raggiungere a questo indirizzo:
http://www.ntecs.de/old-hp/uu9r/lang/html/lang.en.html.
Per farmi perdonare delle numerose toppe che sicuramente avrò preso nel Cyberenigma :D vi mando alcune immagini che, se vi piacciono, potrete usare per qualche vostro articolo.

Netrunner "The Captain"
http://danieleargento.cjb.net

Prova freeHACKnet!

HJ non è solo un sito! Con noi hai la possibiltà di avere un indirizzo email gratuito del tipo nomechevoglio@hackerjournal.it e la possibilità di collegarti ad internet in maniera sicura. Se non ne hai ancora approfittato corri sul sito!

Dati per la connessione

Numero telefonico per la connessione: 7020005073

Username: la tua email (nome@hackerjournal.it)
Password: la tua password

Server SMTP: smtp.hackerjournal.it

Server POP3: pop3.hackerjournal.it

Server NNTP: news.hackerjournal.it
Server FTP: ftp.panservice.it

Assistenza tecnica:
info@hackerjournal.it

Ricordiamo che l'e-mail si attiverà quando riceverà il primo messagio... quindi per attivarla basta mandare un e-mail al vostro indirizzo @hackerjournal.it

SECRETZONE

Nuova Password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troveremo arretrati, sfondi, informazioni e approfondimenti interessanti. Con alcuni browser, può capitare di dover inserire due volte gli stessi codici. Non fermiamoci al primo tentativo!

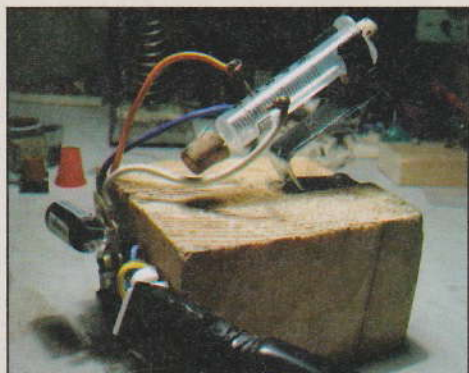
USER: gReCia

PASS: aRRiVo

IL MIO CANNONE ELETTRONICO

Mi ha interessato moltissimo il vostro articolo intitolato "Hacking di una fotocamera con flash" pubblicato nel n. 53 di Hacker Journal e così mi sono costruito anche io il mio cannone elettronico, e funziona benissimo!!! Quindi ho deciso di fare le cose ordinate e di costruirgli una base di legno e vi mando un'immagine come allegato (non è venuta molto a fuoco). Mi piacerebbe se la pubblicaste sulla vostra stupenda rivista, anche per dare una idea a qualcun altro che ha avuto il mio stesso interesse.

Alessandro – "Ilgeniere"

Ciao Alessandro!
Non sei il solo. In parecchi ci hanno scritto, e hanno scritto all'autore, chiedendo spiegazioni, suggerendo altri utilizzi... come akira-1 che vorrebbe invece applicare il tutto a un motorino elettrico. Per quale scopo? Attendiamo le sue prove. Così anche Andrea, che dice "Mi sono divertito molto a creare il cannoncino con la macchina fotografica che avete proposto su HJ n°53".
Ottimo, speriamo che le sperimentazioni continuino e che qualcun altro ci invii qualche foto di altre realizzazioni. StandardBus ci conferma che è lì che sta aspettandoci al varco e intanto ne sta pensando un'altra delle sue... Nel frattempo vi offre anche la foto della sua ultima versione del cannone, con il suggerimento di utilizzare, al posto di un tubetto di plastica, il corpo di una normale siringa da iniezioni, cui avrete (ovviamente) tolto l'ago.

STOP AI DOCUMENTI CONDIVISI

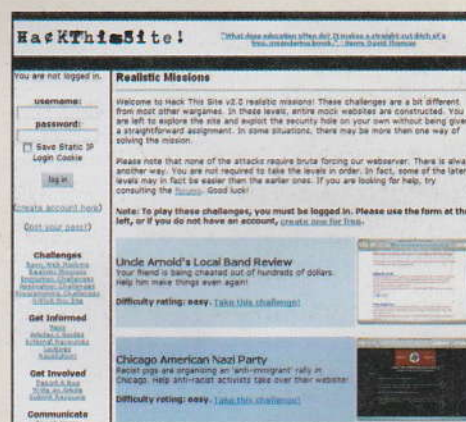
Salve mitica redazione!
Sono scocciato dal fatto che Winndoz XP mi dia sempre la cartella Documenti condivisi nelle Risorse del computer. Non condivido... C'è modo di fargliela piantare lì? Insomma, posso eliminarle definitivamente?

Romolo <Ermajor>

Eccoti la procedura, ma okkio a toccare i registri, sono sempre roba delicata. Fai prima un backup con qualche pulisci registro (Spybot, per esempio).
a) Avviamo l'Editor di registro (Start > esegui > regedit);
b) cerchiamo la stringa: "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\";
c) facciamo clic sinistro e creiamo un nuovo "DWord Value";
d) nominiamo questo nuovo valore in "NoSharedDocuments";
e) facciamo doppio clic su questo valore e settiamolo a 1;
f) chiudiamo l'Editor di registro;
g) riavviamo il sistema.
Già che ci siamo: la finestra "esegui" la possiamo aprire d'un botto con la scelta rapida LogoWindows + R.

E PROVIAMOCI, UNA BUONA VOLTA!

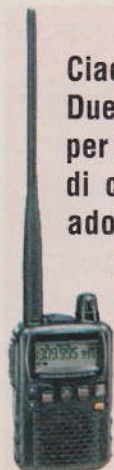
Salve,
vorrei approfondire le mie conoscenze di hacker, però sappiate che sono alle prime armi e non ci capisco tanto. Ho letto e guardato in giro, non sono una volpe con l'inglese, mi piacerebbe provare qualche tecnica di attacco a qualche sito, ma non voglio fare cose illegali. Insomma, vorrei divertirmi un po' aumentando le mie conoscenze teoriche e senza fare danni a nessuno! Possibile che non ci sia un modo facile per capirci qualcosa di più e per soddisfare la nostra passione, che è innanzitutto una curiosità senza fine su questioni tecniche legate all'uso del computer e di Internet? Voi cosa dite?

Paolo

Bingo! Caro Paolo, non scoraggiarti! È esattamente questa "passione che è curiosità" che dobbiamo coltivare! Come, ci stai chiedendo. E non sei solo. Con lo stesso tono della tua riceviamo centinaia di email. La risposta è semplice e concretissima: leggendo, studiando, curiosando... sempre. Ovunque, non smettendo mai. Non sarai una volpe con l'inglese, ma puoi continuare a girare per la rete e cercare

lo stesso di capire. Vedrai che anche la tua comprensione dell'inglese crescerà man mano.
E poi scarica documenti, leggi Hacker Journal con regolarità... chiedi in giro, frequenta i forum.
Infine, o forse subito, fai un salto presso http://www.hackthissite.org/ e registrati gratuitamente. Potrai così scegliere dei giochi di simulazione di attacchi a web server e partecipare ai forum che li accompagnano, esercitandoti nella pratica senza fare danni a nessuno e provando su sistemi che sono lì apposta, per farti "giocare". Anzi, invitiamo tutti quelli che ci proveranno a mandarci i resoconti delle loro scorribande e se facciamo scoperte interessanti e vogliamo spiegare qualche tecnica in modo chiaro e conciso, le pagine di HJ sono aperte anche a queste collaborazioni!

SICUREZZA GSM

Ciao sono Dilan, sono un vostro lettore, intanto vi faccio i complimenti per la rivista: continuate sempre così, l'hacking mi ha sempre affascinato, anche se non ho mai avuto qualcuno che mi spiegasse qualcosa...
Ho due domande: possiedo un palmare Trium Mondo 2003 con Win CE, volendo usare il mio (giocattolo) al massimo, volevo sapere se esiste un altro sistema operativo capace di fare questo.
Volevo anche chiedervi se esiste un modo per ascoltare le telefonate dei GSM. Visto che i tacs non li usa più nessuno.
P.S. Riguardo all'articolo n.54 su Sky avete proprio ragione molti canali sono stati tagliati fuori.

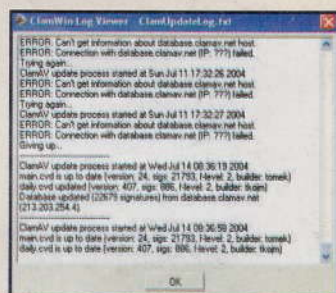
by DILAN

Ciao Dilan.
Due risposte: non ci risulta che per il Trium esista la possibilità di cambiare sistema operativo adottando qualcosa come, diciamo, Linux. Ma speriamo di essere smentiti da qualche lettore. Alla seconda domanda la risposta è doppia. Esistono degli scanner per le frequenze dei GSM. Esistono anche apparecchi _molto_ costosi per intercettare chiamate GSM. Ma bisogna tenere conto che i sistemi di sicurezza che sono tipici della trasmissione GSM derivano dal fatto che la trasmissione non è più analogica, come nei vecchi tacs, ma digitale. La sicurezza della comunicazione è assicurata da algoritmi di crittazione e dall'uso del cosiddetto "spostamento in frequenza" applicati al segnale digitale, che aumentano a dismisura la sicurezza effettiva delle telefonate. Per di più l'anonimato degli interlocutori è altrettanto coperto da un numero identificativo variabile da conversazione a conversazione. Il tutto è quindi molto difficile da scardinare. Su uno dei prossimi numeri approfondiremo l'argomento.

VIRUS? AMMAZZALI CON STINGER

Salve!
Ho letto un articolo, o meglio una lettera di un lettore riguardante Symantec sul numero 54 di HJ. Tutto sommato mi trovo abbastanza d'accordo riguardo la scarsa e qualità di sicurezza offerta da Norton Internet Security (senza dubbio preferisco Zone Alarm e Black Ice). Verso la fine della vostra risposta ho letto che quanto riguarda gli antivirus avete invece preferito ClamWin Antivirus. Data la mia grande curiosità ho voluto subito testare l'efficienza di questo sw... beh per quanto possa apprezzare i programmi freeware non sono ancora riuscito a capire come ci si possa sentire al sicuro con un antivirus che offre protezione contro solamente 22.000 virus circa. A questo punto mi è sorto il dubbio di aver commesso qualche errore o di non aver considerato qualcosa. Insomma potete chiarire questo mio dubbio? Inoltre appena istallato, il programma continua a visualizzare il messaggio "virus database has been updated" nonostante io chiuda la finestra. Concludo con il complimentarmi per la rivista e con il consigliare un antivirus freeware a tutti i lettori (secondo me abbastanza buono):"Antivir 6".

Offdexter87

Caro Offdexter87,
grazie delle tue considerazioni. Riguardo ClamWin, le 22 mila circa sono stringhe che comprendono intere famiglie di virus. Il messaggio di database aggiornato lo dà sempre all'atto del caricamento di Windows, se così l'hai impostato nella configurazione. Possono esserci difetti di gioventù, ma non bloccano il funzionamento del programma.
Già che ci siamo segnaliamo un indirizzo da cui scaricare un antivirus per tutte le definizioni più recenti, utile per una eventuale scansione di sicurezza e in genere risolve le infezioni in atto: http://vil.nai.com/vil/stinger/

NEWS

HOT!

ALTAVISTA ATTACCATA!

Ventinove anni, attualmente dipendente Microsoft, ma dal 1999 al 2000 sul libro paga di Altavista.com. Laurent Chavet è stato arrestato dall'Fbi e rilasciato su cauzione di 10 mila dollari per essere penetrato illegalmente nei computer del suo ex datore di lavoro, recando danni, a quanto pare, per almeno 5 mila dollari all'anno. Il fatto che attualmente lavori in Microsoft, ovviamente, non ha alcun collegamento con la sua nascosta attività di cracker e anche il portavoce della società di Bill si è precipitato a precisare che nulla può trapelare riguardo l'individuo, per un rispetto della privacy che Microsoft adotta sempre nei confronti dei suoi dipendenti. Comunque il rischio a cui sta andando incontro è sicuramente una multa non inferiore ai 250 mila dollari e, se al processo dimostreranno il peggio, fino a cinque anni di reclusione.

PLAYSTATION 3 ALLE PORTE

È stata ribattezzata Playstation 3, ma il nome vero lo conosce solamente Sony. Che per la nuova consolle, il cui lancio sul mercato non è dato di sapere, ma sicuramente non sarà a brevissimo, sta utilizzando il processore "Cell", frutto di una tecnologia sviluppata dalla stessa Sony insieme a IBM e Toshiba. Il nuovo chip, in sviluppo da almeno un paio di anni, offre una potenza gigantesca, pari a quella del supercomputer Deep Blue di IBM. Il nuovo chip pare abbia caratteristiche tali da trattare i filmati con la stessa fluidità con cui un attuale processore può gestire le immagini statiche.
Entro fine anno in Giappone e il 31 marzo 2005 in Europa, sarà presentato al mercato anche un altro gioiellino marchiato Sony: PSP, PlayStation Portable, che vorrebbe dare del filo da torcere al Gameboy Nintendo. Un confronto tutto da giocare.

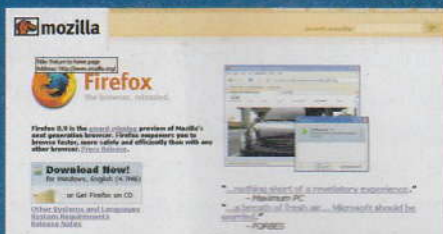
SPARIAMOCI ADOSSO UN TERAHERTZ!

Dieci elevato alla dodici Hertz è la frequenza che servirà per esaminare i turisti agli aeroporti, rendendoli virtualmente nudi come mamma li ha fatti e senza usare i dannosi raggi X. È la nuova tecnologia che verrà sperimentata negli aeroporti di tutto il mondo, per contrastare il fenomeno terroristico. Dietro, un computer analizza il riflesso di tali raggi e ne deduce che sotto il vestito c'è solo una splendida ragazza, oppure stabilisce se un panino sia in realtà un pacchetto d'esplosivo al plastico, un'arma o chissà quale altro materiale sospetto. Sono onde elettromagnetiche piuttosto inesplorate, di cui si sta appunto sperimentando la potenzialità al posto di usare i dannosi raggi X. I risultati sono più che promettenti. Anche perché, a differenza dei raggi X, rispondono in modo molto diverso secondo il materiale che incontrano, dando così la possibilità di capire immediatamente di quale materiale si tratta.

PRENDIAMOCI LA LAUREA ONLINE

Fino al 25 agosto è possibile iscriversi ai test di ammissione per le immatricolazioni al corso di laurea a distanza in Ingegneria Informatica del Politecnico di Milano.
Tutte le info sul sito http://www.laureaonline.it/.
Parecchi gli iscritti ai corsi precedenti e tutti, pare, soddisfatti. La provenienza? Da tutta Italia, ovviamente, ma anche dalla vicina Svizzera.
L'unico obbligo di presenza fisica in un luogo diverso da casa propria è... agli esami: ogni sei mesi ci si deve recare a Como, nella sede del Politecnico, e sostenere l'esame davanti alla commissione.

UN BUCO NE CHIAMA UN ALTRO E UN ALTRO E...

Microsoft non finisce mai di stupire. Windows non ne parliamo. Ma Internet Explorer ha superato se stesso: dopo la falla che ha consentito la diffusione del virus Scob (chiamato anche Download.Ject) a cui da pochissimi giorni Microsoft ha posto rimedio con l'apposita patch, uno studente dei Paesi Bassi avrebbe scoperto un nuovo bug di Explorer, che potrebbe causare problemi analoghi a quelli del bug precedente. È conosciuto fin da gennaio 2004 ed è contenuto in un componente ActiveX chiamato "Application.Shell", utilizzato da Internet Explorer 5.5 e 6.0 su tutte le versioni di Windows. Per ora irrisolto, è innocuo fino a che non viene associato ad altre vulnerabilità e potrebbe consentire l'esecuzione di file eseguibili quali trojan o keylogger. CERT (Computer Emergency Response Team, http://www.cert.org/) è arrivato a sconsigliare, dopo tutti questi allarmi, l'utilizzo di Internet Explorer in favore di browser alternativi, tipo Opera e Mozilla. In una nota si legge inoltre di adottare la precauzione di disattivare ActiveX, Visual Basic Script e JavaScript. Siamo arrivati al punto che perfino un giornalista della rivista Slate, di proprietà di Microsoft, ha raccontato di avere abbandonato Internet Explorer dopo la diffusione di Scob e di avere scelto Firefox (http://www.mozilla.org/products/firefox/) , browser decisamente meno vulnerabile.

UN MILLIMETRO DI SPESSORE TUTTO DA LEGGERE

Bellissimo. È un prodotto Sharp che non vedremo prima del 2007, ma che ha tutte le caratteristiche per diventare un oggetto di culto e, chissà, il vero libro dei prossimi anni. Montato su un supporto trasparente, è l'e-book dei nostri sogni e potrebbe definitivamente sostituire la carta. Funziona senza retroilluminazione per la caratteristica dello schermo impiegato che appare assolutamente analogo alla carta tradizionale, ma con una capacità di riflettere la luce giusto sufficiente per rendere la lettura confortevole. A colori, sarà facile collegarlo alla rete per trasferire al suo interno le pagine di qualunque tipo di lettura vogliamo affrontare: dal libro sull'hacking al quotidiano preferito, passando per il fumetto dell'uomo ragno.

STRATELLITE, NON SATELLITE, WIFI

Stanchi dei normali HotSpot WiFi che non sono mai sufficientemente potenti da darci segnale appena appena ci allontaniamo da casa, ecco venire in soccorso gli Stratelliti della Sanswire.com. Ne piazziamo uno a 20 mila metri di altezza, appena sopra le rotte degli aeroplani, e lui sta lì, forte del suo sistema GPS che lo mantiene in posizione. Intanto trasmette segnale WiFi a tutta la zona sotto di lui dove, presumibilmente, abbiamo piazzato casa nostra. L'ampiezza della zona coperta dal segnale? Circa grande come lo stato del Texas, sia in download che in upload.
È alimentato dalla luce del sole e può arrivare così in alto perché possiede un serbatoio di plastica resistentissimo che abbiamo provveduto a riempire di una miscela di elio e idrogeno. La forma è poi stata studiata per reagire contrastandoli ai venti e alle diverse pressioni a cui è sottoposto a quelle altezze. Insomma, un progetto capace di fruttare parecchi miliardi di dollari... se decollerà.

BATTERIE VERY STRONG!

In attesa delle batterie combustibili, che promettono durate enormemente più lunghe rispetto alle attuali, ma che sono ancora in fase di studio, dal primo di agosto saranno sul mercato le nuove batterie stilo di Sanyo, alla "lega di superlattice". Questa è una nuova combinazione chimica che sostituisce l'attuale polo negativo delle batterie al Nichel Metallo Idruro (NiMH). Cosa ci guadagniamo? 2500 mAh/Min per la dimensione AA. Attualmente la più alta capacità disponibile sul mercato per batterie al NiMH di questo tipo.

HOT!

RICORDI DAL FUTURO

Passato futuro: il nuovo tempo verbale che sembra avere creato Pokia, una società che ha preso le vecchie cornette telefoniche e le ha applicate al cellulare. Follia pura? Si, ma originale. Vogliamo mettere l'effetto di sentire la musichetta preferita della suoneria e tirare fuori dalla borsa una cornetta stile primi novecento, tutta ottone e coni arrotondati? Un modo come un altro per dire basta alla ultraminiaturizzazione spinta in look fantascientifici: vogliamo un bel ritorno al passato.

GUARDA CHE MUSICA!

Gli occhiali da sole con integrato un lettore MP3, come ho fatto a non averci pensato per primo! Li ha indossati per primo Lance Armstrong, durante il giro di Francia. In due versioni, da 128 e 256 MByte, possono riprodurre file MP3 e WMA con una autonomia di circa sei ore e i comandi di volume e riproduzione traccia inseriti direttamente nella montatura frontale. Sono stati battezzati Thump dal produttore: la società Oakley (http://www.oakley.com/), attualmente decisamente trendy.

IG BROTHER IS
ATCHING Y

HOPE 5

Hackers on Planet Earth è arrivata alla sua quinta edizione. Organizzata dalla storica rivista americana 2600, con cadenza biennale, HOPE è il punto di riferimento sociopolitico per gli hacker americani.

ben più di una speranza!

Diversamente da DefCon, HOPE è fortemente orientata ai problemi sociali degli hacker ed è impegnata politicamente per la libertà di parola ed il supporto alle comunità americane ed estere, dove i diritti vengono più facilmente calpestati. Infatti l'ambientazione della conferenza è molto particolare. Simbolismi fortemente politici (di destra e di sinistra) troneggiano sulle pareti ed un gigantesco poster del grande fratello (con una strana somiglianza ad Hitler) ammonisce l'audience che Lui vi sta osservando. A completare tutto il pass che era un bracciale nero da portare al braccio (anche se da buoni hacker l'ho visto indossare al collo, alla gamba alla cintura ed in altri posti troppo difficili da raccontare).

Ex hacker, ora star

Per tre giorni sono sfilati sui due palchi della convention nomi importanti della storia presente e passata dell'informatica. Primo tra tutti Capitan Crunch, l'icona del phreacking degli anni '70, che ha partecipato a diverse conferenze i diverse vesti, la prima come capitano d'industria nella sua campagna contro lo spam, nella seconda, insieme ad un suo vecchio amico, Cheshire Catalyst, per raccontare le imprese e gli aneddoti dei vecchi tempi, ancora insieme a Wozniak come eroe di Steve e successivamente come impiegato numero 13 dell'Apple e infine con Kevin Mitnick quando si è parlato di Social Engineering. In realtà l'intera conferenza ha un filo logico che collega ed unisce tutte queste persone in una unica lunga storia che si snoda per tutte e tre le giornate.

▲ *Capitan Crunch e Cheshire Catalyst. Ne hanno combinate di tutti i colori in giro per mezzo mondo. Ogni tanto segnalavano i problemi a quelli delle compagnie telefoniche che si meravigliavano della loro abilità. Alcuni non hanno mai saputo che loro non erano degli impiegati...*

La situazione cinese

Le sessioni si susseguono sui palchi trattando gli argomenti più disparati, ma ha destato grande attenzione un seminario intitolato "Come funziona la Grande Muraglia cinese", riferito, non senza un certo imbarazzo e dispiacere, all'utilizzo delle tecnologie più avanzate di Cisco per tenere sotto scacco e censurare le comunicazione del popolo cinese. (Cisco non conferma né smentisce la fornitura degli apparti e della tecnologia, ma conferma che sono state sviluppate delle versioni di firmware con delle feature particolari per la Cina) Esiste infatti una lunga lista di IP vietati per il popolo cinese e un'altrettanto vasta lista di parole vietate per i motori di ricer- ▷

...l'intera conferenza ha un filo logico che collega ed unisce tutte queste persone in una unica lunga storia...

2 PAROLE CON MR.2600

2600 è la rivista storica degli hacker americani (e non solo!) e ormai è considerata un vero e proprio riferimento per il settore. Abbiamo fatto due domande a Emmanuel Goldstein, l'editore di 2600:

HJ - Quanti partecipanti ci sono a questo HOPE?

2600 - Oltre duemila persone hanno pagato 50 dollari per questa tre giorni, un risultato veramente interessante.

HJ – Ha ancora senso con Internet organizzare queste manifestazioni?

2600 – Sì è molto importante il contatto fisico e vedersi in faccia aiuta. Specie in questi momenti bui in cui la nostra libertà è sotto attacco come non lo è mai stata!

ca. È interessante vedere come i 18 Gigabit della connettività cinese passino tutti attraverso lo stesso router e come questo si occupi di bloccare le connessioni da e per gli IP vietati. È altrettanto interessante come trasferendo un qualsiasi pacchetto che contenga la parola GET ed un termine vietato un apparato due hop dopo il primo router provveda a bloccare la connessione ed inserire l'IP in una lista di punizione per circa 20 minuti. Una altro effetto interessante, sempre gestito durante il terzo hop all'interno della rete cinese, è il DNS poisoning. Ovvero chiedendo L'IP di un server il cui nome o IP è sulla lista nera si ottengono due risposte: una immediata e sbagliata dall'apparato governativo, ed una seconda, ormai tardiva, dal DNS reale. Questo sarà un grosso problema se Verisign vorrà aggiungere un root DNS all'interno della Cina, perché tutte le richieste per quel DNS nella lista nera effettuate anche al di fuori della Cina daranno risultati sbagliati...

▲ Count Zero presenta il nuovo corso di CDC fortemente ispirato all'ACTIVism, che richiede a tutti gli hacker del mondo di collaborare attivamente per la difesa e la conquista dei diritti civili in tutto il mondo. Per Internet la situazione in Cina è veramente drammatica!

Il condor

Ma tutti durante il primo giorno aspettavano l'ospite d'onore: Kevin Mitnick! Kevin non aveva potuto essere presente alle due conferenza precedenti perché ancora in carcere nel 2000 e sotto sorveglianza nel 2002 e quindi la sua presenza ad HOPE è stata anche un modo per celebrare la completa libertà ritrovata (e l'uscita del nuovo libro intitolato The Art of Intrusion).
Kevin in quasi due ore ha ripercorso la sua intera storia, dalla giovane età fino alla sua recente scarcerazione. Il pubblico lo ha ascoltato in silenzio rumoreggiando quando Kevin si è soffermato sui momenti più dolorosi della sua esperienza, chiuso per oltre otto mesi in isolamento totale: 23 ore e mezzo in una cella da solo e mezz'ora di aria in uno spazio altrettanto ridotto, in manette anche per andare dalla cella alla doccia.

▲ Capitan Crunch - Kevin Mitnick - Emmanuel Goldstein: un terzetto formidabile, che rappresenta la vecchia e la nuova guardia dell' hacker, sotto l'ala protettrice dei media.

Il secondo giorno

Il secondo giorno della conferenza l'attenzione era centrata su Steve Wozniak (the Woz). Steve ha raccontato all'auditorio le sue esperienze giovanili come Hacker e come ingegnere; Woz è da sempre stato un appassionato di scherzi ed ha raccontato come fosse stato possibile combinare la sua passione per l'elettronica con la realizzazione di piccoli sistemi per disturbare la TV e costringere lo sfortunato di turno a svolgere lo spiacevole ruolo di antenna umana: "[accendo il disturbatore] no più a sinistra [spengo] sì così va bene [il tipo si muove, accendo] no ora non si vede ... prova in punta di piedi [spengo] sì rimani così che va benissimo [come la vittima si muove accendo e così via]".

Ma quello che tutti aspettavano era la storia ed il debutto dell'Apple I e II. Tormentato dalla possibilità di continuare

a lavorare con HP, Woz aveva tentato di produrre l'Apple I per l'HP stessa che lo aveva definito "unmarketable" [impossibile da vendere] e gli aveva rilasciato una liberatoria per poterlo commercializzare per conto proprio. Convinto da Steve Jobs (che non aveva esitato a ricorrere al supporto dei parenti ed amici per convincere Woz a lasciare HP per fondare Apple) alla fine cede, anche di fronte all'assegno da 25.000 dollari che un negozio locale aveva staccato per 50 Apple I. Woz non è mai stato motivato nelle sue scelte dal denaro, ma aveva una famiglia da mantenere e questa era la sicurezza che lui andava cercando per essere libero di continuare a sviluppare computer. Tutti i progetti dell'Apple I hanno un importante impronta dal Homebrew Computer Club con i cui soci aveva condiviso tutti i dettagli della piattaforma Hardware e Software dell'Apple I e successivamente anche quella dell'Apple II. Per quanto riguarda l'Apple II, Woz aveva cerato di vendere i progetti alla Commodore ed alla Altair ma entrambi avevano rifiutato, ritenendolo fuori dal mercato... Intanto in 3KB Woz aveva sviluppato un Basic (buona parte dei sorgenti sono stati pubblicati sul Dr. Dobbs Journal) ed inserito all'interno dell'Apple II il sistema per la visualizzazione a 8 colori e la grafica a bassa ed alta risoluzione.
Alla fine quando Woz lascia l'Apple ha pochi milioni di dollari: 28 meno altre spese per campagne di filantropia, circa 10 milioni, ed affari andati male (non c'e ironia in questo, altri hanno guadagnato miliardi di dollari...) ma sostiene ancora l'architettura aperta, sapendo che la vera ricchezza e nella sua mente.

▲ *Steve Wozniak da sempre per la piattaforma aperta: Steve Jobs diceva che 2 slot bastavano ma lui ne ha voluti 8 nell'Apple II.*

Adesso Woz lancia una nuova impresa Weels of Zeus che implementa WiFi e rete cellulare per la localizzazione di persone ed apparati.

Molto più preoccupante è stato invece l'intervento di Steve Rambadam. Steve è un investigatore privato elettronico e ha mostrato al pubblico quanto sia facile ottenere le informazioni ritenute private e riservate. In una veloce sessione online, ha mostrato tutta la storia di una povera vittima che si è prestata all'analisi, scoprendo anche una possibile truffa che poteva coinvolgerlo a sua insaputa. Lo stesso nome della conferenza era inquietante "La Privacy, non è più come una volta". È importante notare che le leggi italiane sono molto più robuste e restrittive sulla privacy e quindi uno scenario da Grande Fratello come quello attuale negli Stati Uniti è molto più difficile da realizzare...

L'ultimo giorno

È il giorno di Jello Biafra, un rapper americano con delle chiare idee politiche da portare avanti, particolarmente in sintonia con la visione anarchica o comunque libertaria degli Hacker. Jello dichiara chiaramente la sua avversione al governo Bush, colpevole a suo dire della morte inutile di oltre mille giovani soldati americani, di oltre ventimila civili in Iraq e della crisi che sta attanagliando la nazione. Comunque, tristemente, ripete che non cambieranno le cose con le prossime elezioni visto che anche Kerry (l'avversario di Bush) è della stessa pasta ed a suo tempo è rimasto coinvolto nelle manovre losche dell'amministrazione. "Era bello quando in America esistevano due partiti diversi", ha detto spiegando come a decine di migliaia di cittadini neri e poveri della Florida sia stato a suo tempo impedito di votare inserendoli in modo fraudolento in una lista di persone che ne avevano perso il diritto. (Bush ha vinto in Florida per circa 6000 voti e la popolazione nera e povera non ha votato certo per Bush...).

In chiusura dell'evento un'altra delle conferenze più attese: Social Engineering con Emmanuel Goldstein, Kevin Mitnick e Cheshire Catalyst, che non si sono solo limitati a raccontare simpatici e divertenti aneddoti, ma hanno preferito lasciarsi andare in una incredibile sessione di Social Engeneering dal vivo...

Silvio de Pecher

I LINK PER APPROFONDIRE

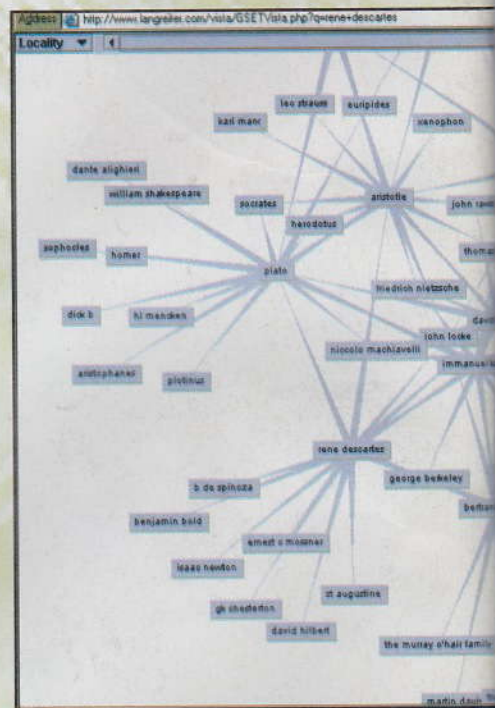
HOPE: www.the-fifth-hope.org
Cina: www.freenet-china.org
Capitan Crunch: http://www.webcrunchers.com/crunch/
Steve Wozniak: www.woz.org
Weels of Zeus: www.woz.com

SOLSTIZIO

Ritratto di che cos'è (e non è) un HACKER dal punto di vista tecnico e morale

▲ *Da Socrate a Leonardo da Vinci, e si potrebbe proseguire fino ad... Hacker Journal!*

Session Start:
Sat Dec 21 03:54:06 2003
Session Ident: Rotten

<wisdom> Ciao.
<rotten> Ciao.
<wisdom> Non capisco il significato del termine hacker.
<rotten> Un hacker è una persona esperta ed entusiasta di qualcosa. Ci sono hacker di musica, di matematica...
<wisdom> Ma allora come mai le riviste per hacker parlano più che altro di informatica?
<rotten> Il termine è usato per lo più in informatica.
<wisdom> Quindi un hacker è una persona esperta ed entusiasta di informatica?
<rotten> Certo! Però ha conoscenze superiori all'utente medio.
<wisdom> In che cosa consistono?
<rotten> L'hacker sa programmare bene e velocemente soprattutto in linguaggi come C e Perl.
<wisdom> Ma questa definizione non è quella della parola programmatore?
<rotten> Un hacker è un programmatore, ma le sue capacità si spingono oltre.
<wisdom> E fino a dove arrivano?
<rotten> Gli hacker sono i più grandi esperti di informatica.
<wisdom> Quindi il più sapiente sui computer non può che essere un hacker?
<rotten> Naturalmente!
<wisdom> Tra le sue capacità c'è anche ottenere il controllo di un server remoto?
<rotten> No, chi compie azioni di questo tipo viene chiamato cracker.
<wisdom> Ma esiste qualcuno che sa più di un hacker sui computer? Se il cracker riesce a fare più cose di un hacker, è lui il conoscitore più grande della rete.
<rotten> No, anche l'hacker ha le capacità per farlo, ma questo non vuole dire che lo faccia.

<wisdom> Ma allora come può un hacker imparare questa arte? Ha le stesse conoscenze di un cracker, ma in che modo le ha apprese? Dalla teoria? Ha comprato libri e libri da hacker e ha studiato?
<rotten> Certo!
<wisdom> Ma esistono libri così che spiegano tutto su come si diventa hacker?
<rotten> No, ma su Internet si trova il funzionamento di praticamente qualsiasi cosa.
<wisdom> Ma come può un hacker conoscere quest'arte solo leggendo manuali in rete? Deve aver pure provato.
<rotten> No, leggendo manuali e documentazioni non ne ha bisogno.
<wisdom> Quindi lui studia solo la teoria.

d'inverno

Dialogo socratico

Questo è un dialogo socratico: rotten si crede dotto e spiega ciò che sa e che crede sia giusto; wisdom corrisponde a Socrate che, fingendosi falso ignorante, fa parlare rotten e dimostra per assurdo che le sue tesi sono sbagliate.
Dimostrare per assurdo significa assecondare le opinioni di una persona e lasciare che creino un paradosso; in questo modo le tesi che si erano credute vere si rivelano false. Rotten pronuncia frasi ispirate al Jargon File e altre che ho letto in IRC, mentre ciò che dice Wisdom è il mio punto di vista.

<rotten> Esatto.
<wisdom> E come può la conoscenza teorica dell'hacker essere più grande della stessa conoscenza teorica, però del cracker, che ha anche conoscenza pratica?
A meno che anche l'hacker possegga conoscenza pratica.
<rotten> Giusto.
<wisdom> E come può averla, senza aver mai provato?
<rotten> Provando su macchine sue, senza abbassarsi al livello del cracker, che attacca macchine altrui.
<wisdom> Quindi un hacker dovrebbe possedere una rete con svariati computer suoi.
<rotten> Già.
<wisdom> Non penso che chiunque si possa permettere una spesa di questo tipo.
<rotten> Ne bastano due, uno da cui preparare l'attacco e uno che lo riceve.
<wisdom> Ma potrebbe provare solo con uno, massimo due sistemi operativi e come può diventare esperto anche di altri?
Dovrebbe avere una decina di hard disk, oppure due hard disk capienti assai partizionati. In ogni caso è una spesa. Quindi una persona non può diventare hacker a meno che non sia ricca?
<rotten> Certo che sì...
<wisdom> E per poter provare un semplice attacco man-in-the-middle dovrebbe avere almeno tre computer. Ma come poter imparare ad aggirare un firewall senza avere un quarto computer collegato a Internet e quindi di un quinto esterno alla rete?
<rotten> Però così facendo un hacker acquisirebbe più conoscenze di un cracker, nel pieno rispetto delle leggi.
<wisdom> Ci sono cose che non si imparano sui libri o nella propria rete. Capire perché ti hanno beccato, dove hai sbagliato, come migliorare, nozioni dovute all'esperienza e che costano rischio.
Perciò, o l'hacker sa meno di un cracker e quindi è inferiore tecnicamente, oppure l'hacker è una persona che ha l'abitudine di superare i suoi limiti cercando di ottenere il controllo su server remoti sempre più protetti.
È illegale; tuttavia, così come esistono hacker devastatori, ve ne sono altri che avvertono gli admin delle falle sui server.
Distinguiamoli per la loro moralità, non per il semplice essere hacker.

Session Close:
Sat Dec 21 04:22:31 2003

Witch_blade
www.selphy.tk
& www.blackserver.it
witch_blade@libero.it

Wine: Windows su

Con un pochino di intraprendenza e il software giusto, possiamo eseguire programmi per Windows su Linux e avere il meglio dei due ambienti

Quanti programmi ci sono per Windows! Se solo funzionasse un po' meglio, costasse meno e fosse un po' più moderno. Sarebbe un sistema ideale.

Che gran sistema operativo Linux! È free, open source e fa imparare un mare di cose. Certo che qualche volta farebbe comodo avere i programmi che girano su Windows. Ed ecco che c'è un sistema per avere i vantaggi di entrambi i Sys. Op. nello stesso momento: Wine (http://www.winehq.com).

Tecnicamente, Wine è una implementazione delle API (Application Programming Interfaces, interfacce per la programmazione delle applicazioni) di Windows sopra Unix e sopra il sistema X (http://www.xfree86.org/). Linux è un sistema basato su Unix e quindi Wine permette di fare funzionare programmi Windows direttamente su un sistema Linux. Il software costituisce uno strato di compatibilità, non uno strato di emulazione, che significherebbe prestazioni ridotte.

ACRONIMI E AMBIENTI DI ESECUZIONE

Anche il nome Wine, come GNU, è fatto per essere apprezzato dagli amanti della ricorsività e dei giochi matematici. Wine, infatti, è acronimo di Wine Is Not an Emulator (Wine non è un emulatore. A proposito, chi sa dire che significa GNU?). A parte i giochi di parole, però, il messaggio è importante. Indica che i programmi Windows non funzionano su uno strato di emulazione; Linux, cioè, non perde tempo a fare finta di essere Windows e quindi non butta via risorse di elaborazione. I programmi Windows trovano i puntelli di sistema di cui hanno bisogno. Semplicemente sono puntelli fatti per andare sotto Linux.

Il codice è interamente Microsoft-free e non richiede possesso di Windows. Chi ha Windows comunque può mettere a disposizione di Wine DLL native, che verranno chiamate regolarmente. Il sistema contiene un toolkit di sviluppo, Winelib, per portare sorgenti Linux su Unix e un program loader, un caricatore di programmi, per prendere un binario Windows ed eseguirlo direttamente, non solo su Linux ma su altri sistemi basati su Unix, come FreeBSD o Solaris.

Installare (da maggio) è semplice

Naturalmente bisogna essere su Linux per usare Wine. La prima cosa da fare è scaricare il software da http://www.winehq.com/site/download.

Linux WINE HQ

Le possibilità sono scaricare il codice sorgente oppure scaricare un file binario già compilato. Nel primo caso dobbiamo decompattare il software con

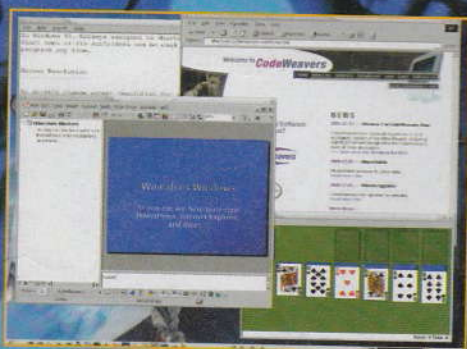
```
tar zxvf Wine-AAAAMMGG.tar.gz
```

Le versioni di Wine si distinguono per data e quindi il comando esatto contiene anno, mese e giorno come appaiono nel nome del file al posto delle maiuscole.

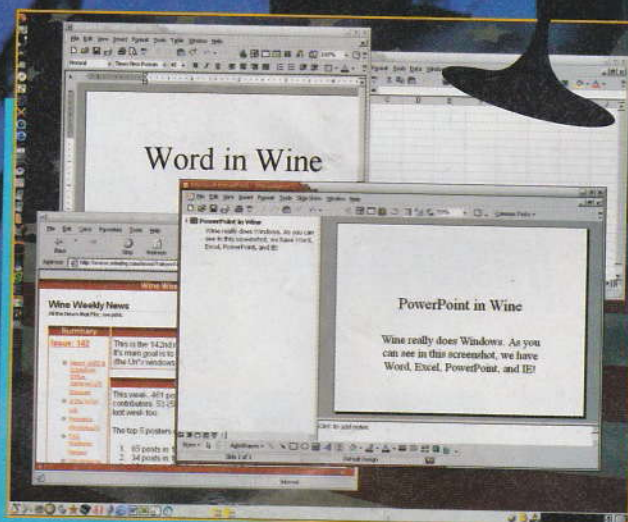
Si crea una nuova directory. Entriamoci e digitiamo:

```
./configure && make depend &&
make && su -c "make install"
```

Se invece abbiamo scaricato un binario, sarà un pacchetto RPM o altrimenti verrà preso da un qualche comando automatico. Nella prima situazione il comando da dare, come root, è

```
rpm -iv wine-AAAAMMGG-i386.rpm
```

▲ *Internet Explorer è uno dei programmi Windows che può tornare utile anche in Linux. Con Wine si può eseguirlo*

Nella seconda dipende dalla distribuzione e dal comando. In Debian, per esempio, sarebbe

```
apt-get install wine
```

Office su Linux? E' possibile!

INSIEME, CONTEMPORANEAMENTE

Perché mettersi su Wine quando si può partizionare con poca fatica il disco rigido e avere una partizione Windows e una partizione Linux? Facile. Il computer può usare solo un sistema operativo per volta. Se funziona Windows, non si può avere Linux senza riavviare e viceversa. Wine è un sistema ingegnoso per fare funzionare i programmi Windows anche se sotto il cofano è in azione Linux.

Da maggio 2004 in avanti Wine crea da solo una directory ~/.wine che contiene quanto necessario al funzionamento generale, compreso un finto disco Windows, la mappatura dei dischi e il resto. La configurazione è pressoché automatica. In compenso è rimasto il vecchio comando wineprefixcreate per chi preferisce fare da sé anche ora che non è più obbligatorio.

▲ *Non va sempre così di lusso, ma anche molti giochi per Windows accettano di funzionare con Wine.*

Per associare una qualunque directory a una mappatura Windows si applica il comando

```
ln -s /mnt/miodisco
~/.wine/dosdevices/d:
```

Che mapperà qualsiasi cosa corrisponda a /mint/miodisco su un finto disco Windows d:.

Come sempre, tutte le informazioni sono contenute nel comando

```
man wine.conf
```

Tutto chiaro? Sotto con Wine!

Nyarlathotep
nyarlathotep@hackerjournal.it

Libertà di XOR?

È interessante chiedersi se il copyright regge anche dopo, o nonostante, una trasformazione matematica di contenuto digitale

Supponiamo di prendere due file binari protetti da copyright e di fonderli insieme prendendoli, bit dopo bit, come argomenti di una funzione logica XOR.
Ne risulta un terzo file che non contiene alcuna informazione effettivamente presente nell'uno o nell'altro file. Questo terzo file è protetto da copyright? E se sì, chi detiene il diritto di copia?

Il terzo file certamente non è una copia diretta di un'originale o dell'altro; i rispettivi contenuti sono veramente diversi.
Non è neanche una derivazione del primo o del secondo file, dal momento che non ne contiene alcuna parte riconoscibile.
Resta però il fatto che, chiamando un'altra funzione XOR avente come argomenti il terzo file e uno dei due originali, si ottiene immediatamente l'altro originale.

Prendiamo 2 file protetti da copyright e fondiamoli assieme. Il nuovo file è sotto copyright anch'esso?

Si sa che il tema del copyright, applicato al mondo digitale, crea grossi problemi, e questa è una delle tante domande possibili che complicano il quadro. Ci sono strumenti open source che permettono di approfondire tali considerazioni, come Monolith (http://monolith.sourceforge.net/).
Monolith è disponibile per qualunque sistema operativo ed essenzialmente calcola l'XOR di due file a nostro piacimento, scrivendo come risultato un terzo file con estensione .mono. Il concetto sopraesposto, tradotto in pratica.

La discussione verte intorno a due estremi. A uno appartiene chi sostiene il copyright a oltranza (partendo dal file originale quello che si ottiene è sempre, in un modo o nell'altro, un derivato). All'altro estremo stanno quanti sostengono che, essendo originale e file XORato del tutto dissimili, non si vede come uno possa trasmettere il diritto di copia all'altro.

MONOLITH

▲ Monolith, programmino a base di XOR per sperimentare i temi delineati in queste due pagine, recuperabile per qualsiasi sistema operativo a http://monolith.sourceforge.net.

//Copertina originale della "Caccia allo Snualo" di Lewis Carroll

Poema in versetti
Libero da copyright

XOR, IL RIMESCOLATORE

Come altre funzioni logiche, anche XOR accetta due bit in input e restituisce un terzo bit di output in funzione di com'erano i due bit di partenza. Lo schema del suo funzionamento è questo:

BIT INPUT 1	BIT INPUT 2	RISULTATO
0	0	0
0	1	1
1	0	1
1	1	0

Se ascoltiamo una canzone alla radio, la fischiettiamo, andiamo a casa, la suoniamo sulla chitarra e registriamo la nostra esecuzione, quando è avvenuta la violazione del copyright?

C'è da un po' chi ha ragionato sul discorso e ha iniziato a mettere in piedi un sistema alternativo e inefficiente, ma ingegnoso, di distribuzione sicura di file. L'idea è creare depositi di file di 128K detti pad. Ogni pad in sé non contiene assolutamente niente di intelligibile, ma se per caso si combinano più pad insieme tramite XOR, ecco che all'improvviso dentro i pad appaiono informazioni. Nessun pad contiene interamente le informazioni suddette, che sono distribuite in modo arbitrario dentro i pad. La cosa interessante non è tanto che un file possa venire nascosto o spezzato o confuso; è il fatto che a un certo punto le persone possono trasmettere o conservare pad senza sapere minimamente che cosa c'è dentro essi e senza possibilità di saperlo.

Il cervello somiglia molto a un encoder MP3: è relativamente efficiente, perde per strada qualcosa del segnale e se uno si concetra riesce ad avere un bitrate elevato.

Qualche utente più furbo – o più attento a queste problematiche – andrà oltre e, mediante XOR, creerà pad visibilmente innocenti. Qualcosa che, XORed nel modo giusto, generi una copia della Caccia allo snualo di Lewis Carroll, o un'incisione della Divina Commedia del Doré… qualcosa che sia assolutamente libero da copyright. O informazioni libere come una raccolta di decimali di pi greco (3,14159) piuttosto che una serie di Fibonacci (1, 1, 2, 3, 5, 8, 13, 21, 34…). Interrogato eventualmente da un giudice circa i pad in suo possesso, mostrerà che portano a informazioni assolutamente innocue, che non è vietato divulgare, né XORare.
Il tema resta controverso. L'importante è non fare niente di illegale… e diventarne più consapevoli.

Kurt Gödel
kurtgoedel@hackerjournal.it

Non è mai per CASO

Generare numeri perfettamente casuali sta a metà tra la scienza, la creatività e l'arte, e serve per un sacco di cose

▲ Vecchie lampade psichedeliche anni Settanta adibite alla produzione di numeri casuali in un laboratorio.

Tutta una serie di programmi che sta nel nostro computer, in un certo senso, imbroglia. Sono i programmi che tirano i dadi, giocano a carte, creano mappe e svolgono qualsiasi altra attività casuale. Non è casuale per niente! I computer infatti sono solo capaci di creare numeri pseudorandom, che sembrano estratti a caso ma finiscono per ripetersi prima o poi, anche se a un esame superficiale soddisfano il nostro bisogno.

È difficile dire se una serie di numeri o qualunque altra cosa sia casuale, anche perché non sappiamo bene che cosa voglia dire! Per esempio, sappiamo che la serie dei decimali di pi greco (3,14159…) è infinita, ma non sappiamo se in qualche punto della sua sequenza c'è una ripetizione o meno. Quando tiriamo una moneta o lanciamo un dado non possiamo essere perfettamente sicuri che il risultato sia veramente imprevedibile. Però qualche indizio lo abbiamo.

Per esempio, una sequenza random deve essere incomprimibile. Se è lunga cento byte, non c'è modo di descriverla in meno di cento byte. Al contrario, una sequenza come 1 2 4 8 16 32 64 128 256 512 1024 2048… si può descrivere brevemente come "le potenze intere positive di 2" e non è certamente casuale.

Si sono trovati diversi sistemi per generare numeri casuali a piacere e fortunatamente possiamo usarli anche noi senza bisogno di essere scienziati, nei nostri programmi oppure semplicemente quando servono.

O per curiosità.

◄ Il cilindro nero appoggiato al computer contiene un sensore CCD che cattura immagini di fondi neri, da cui viene estratto rumore di fondo convertito in numeri casuali. Non è affascinante?

L'11 SETTEMBRE:

Random.org

http://www.random.org

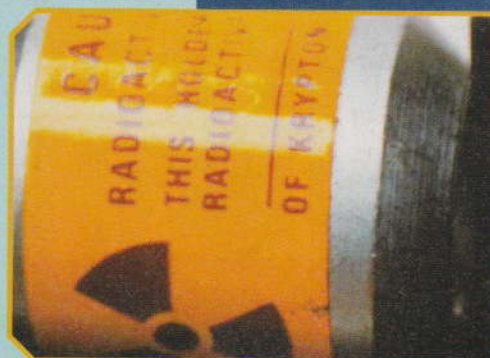
Una radio è sintonizzata sul nulla e diffonde solo rumore atmosferico. Il rumore viene passato a una workstation SPARC Sun tramite la sua porta microfono e campionato come segnale audio mono a una frequenza di 8 kHz. I primi sette bit di ogni campionamento vengono scartati e il resto va a formare un flusso di bit ad alto valore di entropia. Si possono estrarre numeri casuali direttamente dal sito, oppure interrogare il loro server con il giusto programmino via HTTP, SOAP o CORBA. Il sito ospita il codice sorgente di decine di client già pronti.

Entropy Pool

http://random.hd.org/index.html

Mette insieme le serie casuali da più fonti tra cui processi locali sui loro dischi e accessi a pagine Web. La versatilità è poca; dal sito si possono solo scaricare insiemi di bit random. In compenso il software è Java e funziona dovunque.

◄ *Non solo software: questo aggeggino USB serve apposta a generare numeri veramente random. Lo si trova sulla pagina http://www.araneus.fi/products-alea-eng.html.*

▲ *Immagine in falsi colori delle "foto" casuali prodotte dalla LavaCan, lo strumento da cui nascono i numeri random del progetto LavaRnd*

◄ *Krypto-85. Decade in modo meravigliosamente random (basta stare abbastanza lontani).*

HotBits

http://www.fourmilab.ch/hotbits/

Ricava numeri random a partire dal decadimento radioattivo di una capsula di Krypton-85, il cui flusso di particelle viene captato da un contatore Geiger. La produzione di bit random è relativamente lenta e quindi, richiedendo grandi quantità di dati, il sito risponde attingendo a un archivio. Ma il grado di casualità sembra molto buono.

LavaRnd

http://www.lavarnd.org/

Di tutti i sistemi per produrre numeri casuali, questo ha la storia più curiosa. Discende da un vecchio progetto SGI in cui la casualità derivava dall'osservazione di una lava lamp, le lampade psichedeliche anni Settanta piene di un fluido colorato che eccitato dal calore fluttuava lentamente dentro la lampada stessa. Da quel progetto è nato questo, dove invece i numeri casuali vengono prodotti campionando fotografie effettuate a obiettivo coperto.
Tutto il progetto è open source ed è possibile usare il software di LavaRnd per pilotare una propria webcam addetta alla generazione di numeri random.

Vediamo chi è capace di mandarci per primo un programmino che genera numeri casuali e, per esempio, lancia un dado immaginario a sette facce, servendosi degli strumenti messi a disposizione dai siti citati. L'indirizzo a cui scrivere è guestbook@hackerjournal.it

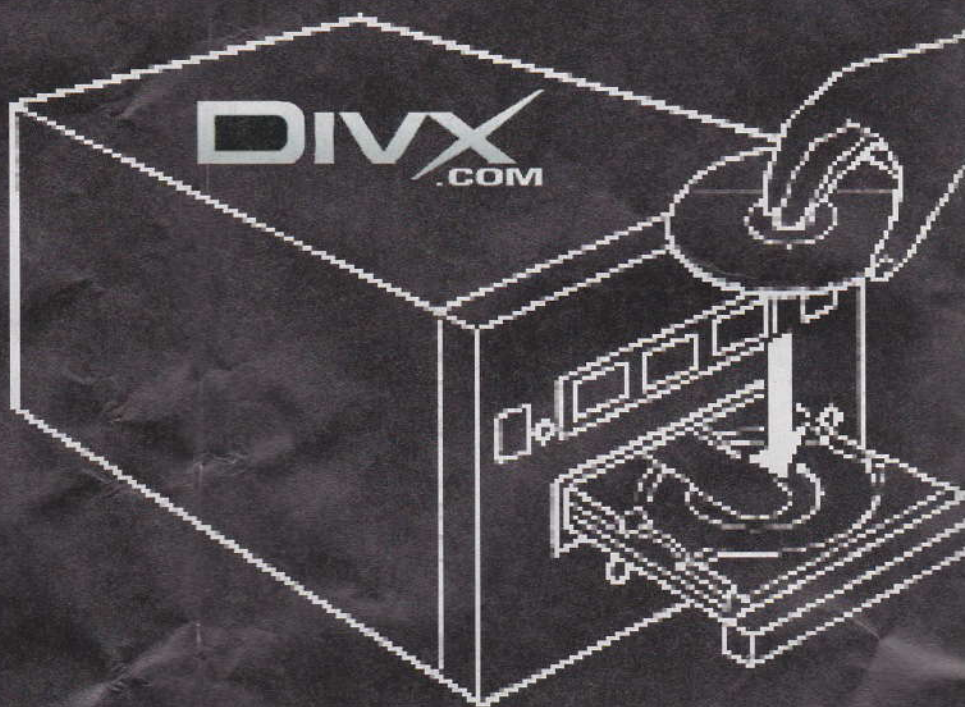
Kurt Gödel
kurtgoedel@hackerjournal.it

▲ *A HotBits usano il decadimento radioattivo per creare numeri casuali, e tengono il materiale radioattivo in questa stanza: una ex cisterna con pareti di calcestruzzo spesse un metro.*

distorsione nella Forza?

Diversi ricercatori sostengono che l'11 settembre 2001 si sia registrata una qualche anomalia nei meccanismi di generazione di numeri random. Secondo i log di random.org non sembra che sia così; ma continua il lavoro di organizzazioni come il Global Consciousness Project (**http://noosphere.princeton.edu/**) che ricercano una specie di coscienza universale alla base di questi fenomeni, quasi esistesse la Forza della saga di Guerre Stellari.

Video al MASSIMO

Come facciamo a vedere un DVD sul computer e magari a ripparlo dentro un singolo CD? Qualunque sia la procedura, c'è di mezzo un codec

La parola codec nasce dalla funzione di coding e decoding, codifica e decodifica. Il codec è quel componente software capace di interpretare il formato dei file video (o audio, o altro) che arrivano sulla nostra macchina e leggere, o scrivere, il formato suddetto.

Il mondo dei codec è in perenne fer-

Uno dei programmi che supporta più codec è VideoLAN Client, disponibile per Windows, Macintosh e Linux a http://www.videolan.org

CODEC PER TUTTI I GUSTI

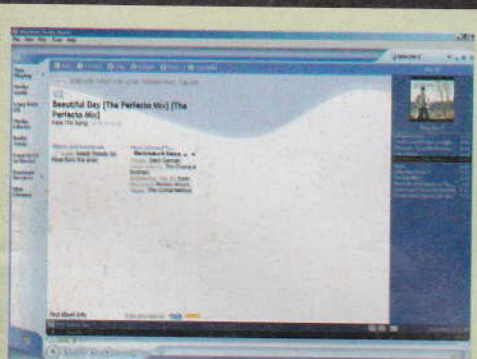
Non sono e non possono essere tutti, ma sono la maggior parte. Quando abbiamo a che fare con video o audio, quasi certamente stiamo usando uno di questi codec.

CODEC VIDEO PER IL WEB

- **Sorenson Video** - qualità alta, richiede un computer potente per riprodurre video su CD
- **RealVideo (Standard)** - codec principale di RealVideo/RealMedia
- **RealVideo (Fractal)** - codec ClearVideo per RealVideo
- **H261** - videoconferenza di bassa qualità
- **H263** - videoconferenza di media qualità
- **MPEG-4** - video ad alta qualità
- **Photo-JPEG** - fotografie
- **ClearVideo** - qualità media, richiede un computer veloce
- **VDOLive** - streaming via server; scalabile
- **Lite VDO** - streaming senza server

CODEC VIDEO PER CD-ROM/DVD-ROM/CHIOSCHI MULTIMEDIALI/PRESENTAZIONI

- **Cinepak** - qualità media, funziona anche su computer vecchi
- **Sorenson Video** - qualità alta, richiede un computer veloce
- **DivX** - qualità alta, spesso usato per ridurre i DVD a dimensioni accettabili
- **Eidos Escape** - qualità alta, richiede un computer veloce
- **Power!Video** - qualità alta, richiede un computer veloce
- **Indeo 3** - qualità media, funziona anche su computer vecchi
- **Indeo Video Interactive (4, 5)** - qualità alta, richiede un computer veloce
- **Apple Video** - molto veloce ma qualità bassa (usabile per i test)
- **MPEG-1** - qualità alta, richiede hardware speciale o un computer veloce
- **MPEG-2** - qualità alta (DVD), richiede hardware apposito
- **Apple Animation** - lavora con i dati su disco rigido e permette riproduzione a tutto schermo a

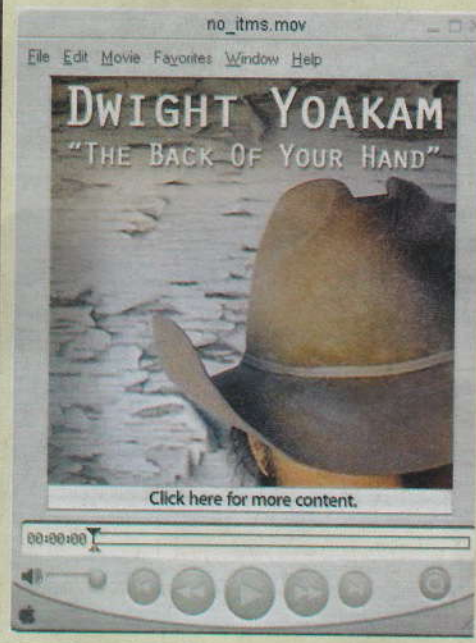
con il CODEC giusto

▲ *Windows Media Player supporta numerosi codec, ma è chiuso e non aggiornabile da parte dei programmatori indipendenti.*

mento; per esempio e per dare una notizia piuttosto attuale, il DVD Forum ha ratificato l'inclusione dell'Advanced Video Codec (AVC) H.264 nel formato dei DVD di prossima generazione, detto High Definition o HD. H.264/AVC è stato sviluppato insieme dal Moving Picture Experts Group, altrimenti detto MPEG, e l'Unione internazionale delle Telecomunicazioni (ITU) e fa parte delle specifiche dello standard MPEG-4. Una cosa bella è che il tutto è interamente basato su standard aperti. H.264 è estremamente scalabile, ossia si adatta bene a qualunque tipo di requisito di trasmissione. Quindi funziona tanto per la televisione ad alta definizione (1.920 x 1.080 punti) quanto per mandare video sui minischermi dei cellulari. Più o meno tra un anno vedremo H.264/AVC un po' dappertutto. Lo standard completo è descritto nel documento Overview of the H.264/AVC video coding standard reperibile all'indirizzo http://www.ebu.ch/trev_293-schaefer.pdf.

I codec hanno natura modulare e sono adatti per essere inseriti nelle architetture di trattamento dei media aperte ed espandibili a piacimento, come per esempio QuickTime. In altre architetture, come Windows Media o Real, non è invece possibile intervenire e bisogna attendere che siano i loro proprietari (Microsoft e Real Networks, nello specifico) a inserire i nuovi codec e allargare così le capacità di lettura dell'architettura.

Questo spiega che cosa succede quando proviamo ad aprire un filmato o un'animazione con il nostro programma di riproduzione preferito e non ci riusciamo. Quasi certamente la codifica è stata eseguita con un codec che il programma non ha a disposizione.

Michele Campovecchio
michele_c@hackerjournal.it

***QuickTime* è una architettura aperta, espandibile con qualunque codec.**

qualità totale su sistemi molto potenti

CODEC VIDEO PER ACQUISIZIONE E HARDWARE SPECIFICO

- **Media 100** - permette l'uso dei file senza hardware di acquisizione
- **Radius VideoVision Studio** - permette l'uso dei file senza hardware di acquisizione
- **Avid Media Composer** - permette l'uso dei file senza hardware di acquisizione
- **TrueVision** - permette l'uso dei file senza hardware di acquisizione
- **DV Camera** - formato tipico delle videocamere digitali
- **Apple Component Video** - per l'acquisizione su sistemi senza hardware JPEG

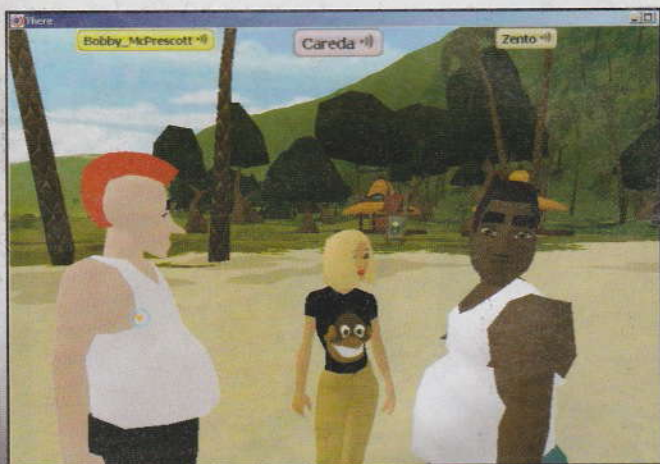
CODEC VIDEO PER CONSERVAZIONE, EDITING E USI SPECIFICI

- **Motion-JPEG (MJPEG)** - editing e conservazione
- **Apple Graphics** - molto simile al formato GIF, per immagini a pochi colori (per esempio schermate di sistema)
- **Apple None** - qualità totale, ma inefficiente
- **Apple Animation** - conservazione a qualità totale
- **Photo-JPEG** - usato per conservazione e trasferimento di file, crea file molto ridotti in dimensioni.

CODEC AUDIO

- **AAC** - qualità alta per il Web, superiore a MP3
- **IMA** - compressione 4:1 (usato nei CD-ROM)
- **MPEG layer III audio** - qualità alta per il Web (anche chiamato MP3)
- **QDesign Music Codec** - qualità alta per il Web con poca banda
- **Qualcomm PureVoice** - parlato per modem a 14.4 kbps
- **G.723** - parlato per videoconferenza
- RealAudio - audio su Web

ABBASSO il Grande Fratello

Il progetto Winston Smith vuole evitare che il Grande Fratello (quello di Orwell, non quello TV) possa diventare realtà

◄ *Un altro modo di essere anonimi è avere un buon avatar*

I sostenitori del progetto Winston Smith credono che le previsioni di Orwell in 1984 si stiano materializzando e sia possibile scongiurare questa ipotesi promuovendo l'anonimato e la cifratura personale come sistemi per tutelare la privacy di ognuno. Secondo il Manifesto che si può leggere sul sito https://remailer.futureworlds.it /pws/index.html, uno degli ostacoli fondamentali per raggiungere l'obiettivo consiste nella scarsa conoscenza e nell'ancora più scarso utilizzo di strumenti difensivi della privacy che invece hanno già grande potenza. Se fossero più conosciuti e utilizzati le minacce alla privacy perderebbero efficacia.

Per questo il progetto intende facilitare la creazione di fornitori di servizi per la privacy diffondendo l'informazione sul know-how e la documentazione necessaria alla costituzione veloce e a costo minimo di server pubblici per la privacy stessa.

Qualcosa di concreto

Fino a qui potrà sembrare che il progetto Winston Smith produca solo parole. Invece ci sono fior di fatti e non pochi. Prima di tutto c'è la docu-

UN NOME DA UN LIBRO

Il Grande Fratello televisivo ha distratto quasi tutte le teste dal personaggio omonimo del libro 1984, scritto dall'inglese George Orwell nel 1948. L'autore ricavò la data, per lui fantascientifica, semplicemente invertendo le ultime due cifre dell'anno di pubblicazione. Winston Smith è uno dei protagonisti del libro, nel quale l'oppressivo dittatore Grande Fratello osserva e ascolta costantemente tutta la popolazione. Smith finirà per opporsi al potere onnipresente e dittatoriale che soffoca ogni tipo di libertà, quando…

mentazione, scaricabile all'indirizzo https://remailer. futureworlds.it/pws/software/PWS.zip, oppure consultabile in forma ben strutturata sul sito. Poi si trovano sezioni di software suddiviso in programmi per la cifratura e programmi relativi al progetto Freenet, con link a programmi disponibili, come GPG, ma anche con puntatori interessanti a software meno noto come Mixmaster o Echolot, sempre con l'obiettivo dell'anonimità e della tutela della privacy.

Come partecipare

Si può voler partecipare al progetto Winston Smith anche semplicemente da sostenitori, senza dover essere per forza coinvolti e senza bisogno di chissà quali conoscenze tecniche. Al team del progetto serve anche gente che abbia voglia di aiutare a scrivere (o a rileggere) la documentazione, piuttosto che testare i programmi e piuttosto che riferire i bug ai programmatori. Si può partecipare al progetto anche solo iscrivendosi alla mailing list e-privacy (https://remailer.futureworlds.it/pws/lists.html). Naturalmente, appena possibile, è giusto farlo in forma anonima!

Winston Smith ha anche un indirizzo email, ws@nym.alias.net. Sosteniamolo e scriviamogli. Anonimamente, per restare persone.

> ***"Chi è pronto a rinunciare alle proprie libertà fondamentali per comprarsi briciole di temporanea sicurezza non merita né la libertà né la sicurezza." Benjamin Franklin***

Sul sito http://www.winstonsmith.info è possibile anche inviare commenti in forma completamente anonima.

Reed Wright
reedwright@mail.inet.it

L'indirizzo

Come mettere la nostra email sul Web in modo

Uno dei sistemi più comuni di nascondere la nostra mail ai motori degli spammer è codificare l'indirizzo come entità HTML. Possibile che uno spambot (i robot degli spammer) riesca a capire che dietro la sequenza di caratteri mailto si nasconda una normalissima scritta mailto…?

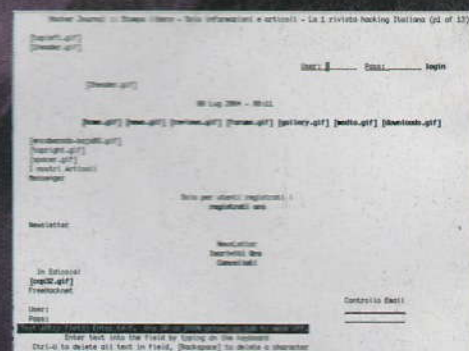
Il problema è che pensiamo troppo a come la vediamo noi e meno a come la vedono loro. A noi quell'intrico di & e # suggerisce confusione e indecifrabilità. In più pensiamo agli spammatori come a dei cretini, dal momento che spediscono mail palesemente cretine. Purtroppo le mail sono cretine, loro no. E ci vuole poco per uno spammer a capire come stanno le cose e studiare una buona espressione regolare che catturi le entità HTML. Come esiste un sistema molto veloce per codificare rapidamente un indirizzo in entità (Fantomas MailShield, all'indirizzo http://fantomaster.com/fantomasSuite/mailShield/famshieldsv-e.cgi), non è difficile programmare l'operazione inversa.

Qualcuno ha pensato di complicare le cose, allora, nascondendo (si fa per dire) l'indirizzo codificato in entità dentro un JavaScript. Una cosa tipo questa:

```
<script type="text/javascript">
<!--
document.write('<a href="mail-
to:&#109;&#105;&#108;&#097;&#
064;&#109;&#097;&#105;&#108;&
#046;&#105;&#116;" title="Indi-
rizzo email codificato.">Scrivi-
mi!<\/a>');
// -->
</script>
```

(che indirizzo è, a proposito?) Tutto bene, molto astuto, ma ci sono due problemi. Il primo è che non è cambiato assolutamente niente per il robot! Infatti la sequenza è la stessa, solo inserita dentro un po' di tag (quelli JavaScript) in più. Lo spambot lo troverà con un miliardesimo di secondo di ritardo, ecco. Secondo problema, i link scritti in JavaScript andrebbero evitati. Pochi lo sanno, infatti, ma più di un utente non usa JavaScript! Tra le categorie a rischio ci sono quelli che usano un browser solo testo, come Lynx (http://lynx.browser.org); chi usa browser normali in azienda solo che per ordini superiori è stato disabilitato; e altri ancora.

Se hai Javascript vedi l'indirizzo reale. Se non hai JavaScript vedrai l'indirizzo Spam Motel, che se sei umano funzionerà comunque, mentre se sei uno spambot ti manderà nel nulla.

◄ *Visto come è semplice convertire un indirizzo email in entità?*

▲ *Lynx, il browser solo testo, disponibile per tutti i sistemi operativi del mondo. Quando non servono le immagini, è anche il browser più veloce del mondo. Caricare solamente l'HTML, infatti, è uno scherzo.*

MASCHERATO

che la leggano solo gli umani. E ci siamo capiti

◄ *Spam Motel (http://www.spammotel.com), il sistema che genera email usa e getta nell'intento di sconfiggere lo spam.*

Se JavaScript va usato, visto che rappresenta un problema di usabilità e Web design, almeno lo si usi bene, per mettere veramente in difficoltà gli spambot. Ed ecco l'idea: unire Javascript e un sistema di indirizzi usa-e-getta con cui gettare fumo negli occhi agli spammer, senza escludere nessuno, tantomeno Lynx. Il sistema lo abbiamo, ne abbiamo parlato nel numero scorso di HJ: è Spam Motel (http://www.spammotel.com). Il suo meccanismo permette di creare tutti gli indirizzi a perdere che vogliamo e buttarli via quando sono spammati.

Adesso serve un pezzo di JavaScript nella sezione <head> delle pagine in cui intendiamo linkare l'indirizzo di posta, destinato a fare un po' di confusione mirata con l'indirizzo vero:

```
<script type="text/javascript">
function offusca_mail()
{
        mail_inizio     =
"mailto:ne0k0n@";
  mail_fine = "urnal.it";
 mail_interno = "hackerjo";
 return mail_inizio + mail_interno + mail_fine;
}
</script>
```

Poi, per creare il link vero e proprio, si combina un indirizzo di Spam Motel con la funzione offusca_mail:

```
<a href="mailto:WGAFJEUYFOQC
@spammotel.com"
onclick="this.href=offusca_mail();
" onMouseOver="window.status=offusca_mail();return true;"
onmouseout="window.status='';return true;">Scrivimi!</a>
```

Qui viene il bello: chi non usa JavaScript, ma soprattutto uno spambot, otterrà l'indirizzo Spam Motel, che per le persone funzionerà mentre manderà a vuoto gli spammatori. Chi usa JavaScript dovrebbe ottenere l'indirizzo vero, il quale, si noti, non è visibile nel codice della pagina, a meno che uno spambot non si metta ad analizzare e ricucire stringhe trovate dentro tag JavaScript. Sono intelligenti, ma non così tanto.
E ho l'impressione che, con il tempo, tendano a rivendere i vecchi indirizzi più che cercarne di nuovi.

Ne0k0n
ne0k0n@hackerjournal.it

Regex Reloaded

Cose da sapere e da scoprire sulla tecnologia che fa diventare maghi del trattamento dei testi

Riparliamo di regex, o espressioni regolari: il sistema per trovare nei testi qualsiasi cosa vogliamo. Intanto salutiamo quelli che hanno scritto a proposito dellíultimo articolo sulle regex pubblicato e non sono più stati menzionati: Buffer Overflow, X-3meí89, DarkLink, Daniele Midi, Nixxo, Jerk, LoRd_MoRo, Roberto Bossola, klaus74 e ahzrael hanno lavorato a spiegare, tra líaltro, che cosa significano i parametri \1, \2, \3 eccetera.

Sono parametri di spostamento e servono a effettuare interventi intelligenti sul testo con le regex.
Se, infatti, comprendiamo tra parentesi tonde i vari termini di una ricerca, essi vengono memorizzati in ordine.

REGEX ALL'INDIRIZZO

Qualche sito dove diventare maghi di regex:

http://it.diveintopython.org/dialect_re.html (in italiano)
http://www.biocomp.unibo.it/piero/corso/note/node69.html (in italiano)
http://www.corsolinux.it/testi/perl/analog/le_espressioni_regolari.jsp (in italiano)
http://www.english.uga.edu/humcomp/perl/regex2a.html
http://www.html.it/perl/perl_11.htm (in italiano)
http://www.lc.yi.org/scribble/scribble_show.php3?sid=226
http://www.regenechsen.de/regex_en/regex_1_en.html
http://www.regular-expressions.info/
http://www.silverstones.com/thebat/Regex.html
http://www.univ.trieste.it/~nircdc/doc/oldunix/DUerm.8.1.html (in italiano)

Esempio: cerchiamo

```
([a-zA-Z]+)( )([a-zA-Z]+)
```

// Le regex o espressioni regolari **sono il sistema per trovare in un testo, anche molto lungo, qualsiasi cosa con estrema precisione e velocità**

o, in italiano, un gruppo di una o più lettere dellíalfabeto maiuscole o minuscole, uno spazio e un altro gruppo simile al primo. Questa regex identificherà stringhe come:

```
Paolo Bianchi
Carla Rossi
Andrea Verdi
```

Occhio alle parentesi tonde: la prima viene memorizzata come \1, la seconda come \2 e via dicendo. Quindi, cercando quanto sopra e sostituendo con \3\2\1, avremo il contenuto della terza parentesi tonda messo al primo posto, il contenuto della seconda (lo spazio) lasciato al secondo posto e, in coda, il contenuto della prima parentesi tonda. Otterremo:

```
Bianchi Paolo
Rossi Carla
Verdi Andrea
```

Se abbiamo un elenco di nomi-cognomi che dobbiamo ordinare alfabeticamente per cognome, le regex facilitano il compito. Certo, si potrebbe fare la stessa cosa con un foglio elettronico (come?), ma un'espressione regolare è elegante e automatica; lavora lei al posto nostro.

Facciamo allora il punto e riassumiamo i metacaratteri principali di regex che abbiamo incontrato. La sintassi è la più standard possibile e può cambiare leggermente secondo gli strumenti e il software usato:

METACARATTERE	DESCRIZIONE	CORRISPONDE A...
.	punto	...un carattere qualunque
[]	gruppo di caratteri	...qualunque carattere presente nella parentesi quadra
[^]	gruppo di caratteri negati	...qualunque carattere non presente nella parentesi. Il segno di caret sta allíinizio dellíelenco dei caratteri negati, come in [^abc].
\	escape	...al carattere e non a un suo eventuale significato. [normalmente apre un gruppo di caratteri; \[indica semplicemente il carattere di parentesi quadra aperta.
?	punto di domanda	...contatore: da zero a uno volte il carattere o gruppo che precede
*	asterisco (star)	...contatore: da zero a infinite volte il carattere o gruppo che precede
+	addizione	...contatore: da uno a infinite volte il carattere o gruppo che precede.
^	caret	...posizione: inizio di una riga
$	dollaro	...posizione: fine di una riga
\<	confine parola	...posizione: inizio di una parola
\>	confine parola	...posizione: fine di una parola
|	pipe	...alternativa: o il gruppo/carattere prima, o il gruppo/carattere dopo
()	parentesi tonde	...insieme: il contenuto viene memorizzato durante líelaborazione della regex
\1	backreference	...rappresenta il contenuto della prima, della seconda, della terza... parentesi tonda.

Un vero problema, o un problema vero

A che servono le espressioni regolari? A compiere magie sui testi, per risolvere problemi reali. Facciamo un salto di qualità, per imparare che le regex non servono solo da sole, ma unite a un pizzico di programmazione fanno miracoli autentici. Purtroppo lo spazio per questo numero è finito. Ma ce nè dell'altro, a pagina 32. Chi avrà il coraggio di cimentarsi nel cyberenigma di questo numero apprezzerà ancora di più i prossimi articoli sulle espressioni regolari!

Barg the Gnoll
gnoll@hackerjournal.it

☐ REGEX SECONDO BUFFER OVERFLOW

Catturare qualsiasi indirizzo email:

```
[a-zA-Z.:_-]*@[a-zA-Z.:_-]*.( [a-zA-Z.:_-]*.)?[a-zA-Z]*
```

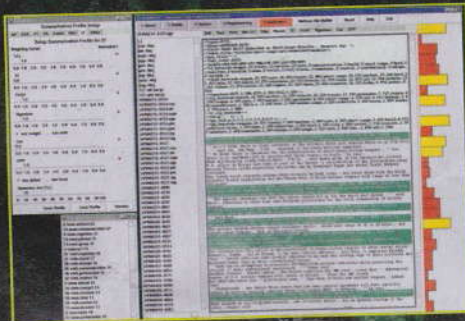
Riconoscere una data nel modo più preciso possibile:

```
((([0-9][0-9][0-9]?[0-9]?[/\.;:_-][13578]|(1[02])|(0[13578])[/\.;:_-][1-9]|(0[1-9])|([12][0-
9])|(3[01]))|([1-9]|(0[1-9])|([12][0-9])|(3[01])[/\.;:_-][13578]|(1[02])|(0[13578])[/\.;:_-][0-
9][0-9][0-9]?[0-9]?))|((([0-9][0-9][0-9]?[0-9]?[/\.;:_-][469]|11|(0[469])[/\.;:_-][1-9]|(0[1-
9])|([12][0-9])|30)|([1-9]|(0[1-9])|([12][0-9])|30[/\.;:_-][469]|11|(0[469])[/\.;:_-][0-9][0-
9][0-9]?[0-9]?))|((([0-9][0-
9]((0[48])|([13579][26])|([2468][048])))|((16|([3579][26])|([2468][048])00)|(([02468][048])|([1
3579][26]))[/\.;:_-]2|02[/\.;:_-]29)|(29[/\.;:_-]2|02[/\.;:_-]((([0-9][0-
9]((0[48])|([13579][26])|([2468][048])))|((16|([3579][26])|([2468][048])00)|(([02468][048])|([1
3579][26]))))))|(([0-9][0-9][0-9]?[0-9]?[/\.;:_-]2|02[/\.;:_-][1-9]|(0[1-9])|(1[0-9])|(2[0-
8]))|([1-9]|(0[1-9])|(1[0-9])|(2[0-8])[/\.;:_-]2|02[/\.;:_-][0-9][0-9][0-9]?[0-9]?)
```

Ma questa non abbiamo provato a verificarla!

Dal linguaggio al C...

Se siamo sufficientemente motivati possiamo programmare qualsiasi cosa!

Alan Turing ci ha spiegato che esistono problemi di cui sappiamo è impossibile arrivare a trovare una soluzione, non importa che computer abbiamo.
Kurt Gödel ha dimostrato che nessun sistema formale (per esempio un linguaggio di programmazione) è esente da contraddizioni interne.
Quello che i programmatori riescono ugualmente a realizzare è stupefacente, come il traduttore da linguaggio C a inglese e viceversa.

▲ *Un compito difficile per un programma? Riassumere un testo e conservarne il significato. Per noi è roba da scuola elementare.*

Si chiama c2txt2c, è stato realizzato da un programmatore finlandese di nome Leevi Marttila e si può vedere (nonché scaricare) a http://personal.sip.fi/~lm/c2txt2c.

Nei progetti futuri di Leevi vi è la produzione di scheletri diversi, per altre lingue oppure per dare stili diversi all'output, dall'umoristico al fantastico e così via. Inoltre è attivo il lavoro su altri lin-

LO SCHELETRO NEL DIZIONARIO

Il tipo di testo comune prodotto da c2txt2c dipende da uno scheletro di linguaggio che viene passato al programma. Eccone un esempio, che lasciamo in inglese perché si apprezzi meglio l'ambiguità (o la similitudine!) tra strutture di programmazione e strutture del linguaggio.

```
for:
{for[s]([expr.1];[expr.2];[expr.3])
[s][compound]} <=>
 {Do next things several times.
Start with this:[s][expr.1]\
 \[s]Does next thing talk about
truth?[s][expr.2]\
 \[s]When you have again done
all, then do this:[s][expr.3]\
 \[s]Here is list of things you
should do:[compound]}
;
```

Quanti sognano un traduttore universale (ovviamente in fase di studio) che semplifichi l'approccio con le belle ragazze di altri paesi?

Ma chi invece avrebbe mai pensato ad un linguaggio che ci permetta di parlare con le macchine così come con le belle ragazze?

▲ I programmatori di avventure e di giochi in cui si passano messaggi al programma si sono sempre trovati ad accoppiare linguaggio parlato e di programmazione.

guaggi di programmazione per ottenere lo stesso risultato. Particolarmente adatto, e primo fra tutti, è ovviamente Perl. Roger Espel Llima ha già realizzato un primo esempio di script in questo senso, visibile a http://www.iagora.com/~espel/pleng.

Per rimanere al corrente esiste una mailing list, cui ci si iscrive inviando un messaggio con subject subscribe all'indirizzo lm+c2txt2c-request@sip.fi.
Come si vede dal semplice esempio che pubblichiamo, la traduzione dal C all'inglese è certamente scolastica. Ma fa un po' impressione pensare che, ritradotto l'inglese in C, tutto il significato del programma rimane invariato. Terremo d'occhio gli sviluppi.

Barg the Gnoll
gnoll@hackerjournal.it

...e viceversa

BANANE, MELONI E BLOWFISH

Dall'algoritmo di cifratura Blowfish:

```
/* DCBA - little endian - intel */
#ifdef ORDER_DCBA
union aword {
  UWORD_32bits word;
  UBYTE_08bits byte [4];
  struct {
    unsigned int byte3:8;
    unsigned int byte2:8;
    unsigned int byte1:8;
    unsigned int byte0:8;
  } w;
};
#endif          /* ORDER_DCBA */
```

Tradotto in linguaggio naturale:

Comment by author: " DCBA - little endian - intel ".
If "ORDER_DCBA" is mentioned, then read next lines.

These briefcases can hold next things:

Treat next things as a compound. There is David code named "word". He likes melons. Move to next person.
There is Thomas code named "byte". Calculate next thing: 4 He likes to carry that amount of bags of cherries. Move to next person.

These big chests can hold these things:

Treat next things as a compound. There is Paul code named "byte3". He likes some bananas. His hands are 8 centimeters wide. Move to next person.
There is Eugene code named "byte2". He likes some bananas. His hands are 8 centimeters wide. Move to next person.
There is Wayne code named "byte1". He likes some bananas. His hands are 8 centimeters wide. Move to next person.
There is Joseph code named "byte0". He likes some bananas. His hands are 8 centimeters wide. Move to next person.

Now I have listed all things that belong to that compound. Now George code named "w" is stuffed full.
Now I have listed all things that belong to that compound. However it won't hold those things at the same time.

That was all things related to that thing.

LA FUNZIONE NON È PIÙ

LA RISPOSTA BASE ERA PIUTTOSTO SEMPLICE, UN BUON INVITO AD AVVICINARSI ALLA PROGRAMMAZIONE. ALCUNE RISPOSTE PERÒ SONO STATE SORPRENDENTI...

UN SOLO RITARDATARIO

Giuseppe De Roma (o sarà de Roma, nel senso di proveniente dalla capitale?) si è meritato il titolo di genio del Cyberenigma del num. 52 , anche se si è preso due settimane di licenza rispetto a tutti gli altri. Complimenti a lui e a tutti quanti sono sempre più bravi a rispettare i tempi di uscita!

NON PERDIAMOCI DI VISTA

Istruzioni per aiutare a pubblicare tutti i partecipanti:

- scrivere nel subject della mail Cyberenigma e il numero della rivista, meglio ancora il titolo del cyberenigma;
- indicare con chiarezza il nickname in fondo al messaggio;
- scrivere possibilmente prima che esca il nuovo numero di HJ;
- usare l'indirizzo di mail che appare nella pagina del cyberenigma.

Per chi rispetta le istruzioni la pubblicazione è certa!

{[TONIC]} IN FORTRAN

```
      INTEGER FATT,N
      READ (5,50) N
50 FORMAT (I1)
      FATT=1
      DO 100 I=1,N
      FATT=FATT*I
100 CONTINUE
      WRITE (6,110) FATT
110 FORMAT(I6)
      STOP
```

Le soluzioni

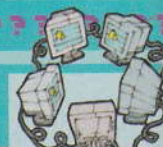
PER TUTTI: La funzione blip da indovinare era il calcolo del fattoriale di un numero. Per esempio, il fattoriale di 6 (scritto 6!) è 6 x 5 x 4 x 3 x 2 x 1 = 720.

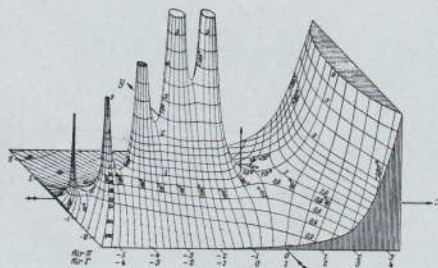
PER ESPERTI: In ordine di apparizione, la funzione era scritta in Visual Basic, JavaScript, Java, Pascal, C, Lisp, Forth, Prolog, Perl, Modula-2 e Python.

PER GENI: Si chiedeva di programmare la funzione blip in modo diverso da quello presentato.

PER SUPER HACKER: Si chiedeva di programmare la funzione blip in modo diverso da quello presentato in uno o più linguaggi mai studiati prima.

Sorridi! Sei anche tu un super hacker!

►Spesso il fattoriale viene programmato usando la ricorsività. Le foto che si rifilettono sulla visiera degli astronauti sono un altro fenomeno ricorsivo.

BLIP

UN MISTERO

AS12-48-7071

Ecco chi ha risposto!

Il primo a spedire una soluzione è stato M3rcuti0, genio (ma dov'è l'allegato? :-)!

Hanno risposto anche (in ordine di arrivo):

349…	Per tutti
m@tted@llo	Per tutti
Gabriele (c'erano undici esempi…)	Per tutti
Derbeer	Per tutti
Simonide	Esperto
Franco Lupi (anche se ci corregge le funzioni!)	Esperto
Ale80	Esperto
bauz	Esperto
Fabio	Esperto
Cplusplus	Genio
Anonymous	Genio
++SiNeRgY++	Genio
Francesco Guatieri	Genio
Benny	Genio
xand	Genio
CaparezzaMC	Genio
CIX	Super hacker!
Daniele Midi	Super hacker!
{[ToNiC]}	Super hacker!
GeminiNero	Super hacker!
Netrunner "The Captain" (buon compleanno!) (per il Morse… prova a rispedire!) (pigro. Bravo lo stesso!)	Super hacker!
Infernet89 (per l'originalità. Bravissimo!)	Super hacker!

Un solo commento: praticamente nessuno ha indovinato tutti i linguaggi di programmazione… ma sono arrivati molti esempi in altri linguaggi ancora, alcuni veramente originali. Bravi e alla prossima!

Barg the Gnoll
gnoll@hackerjournal.it

FATTORIALIZZARE O NON FATTORIALIZZARE, QUESTO È IL PROBLEMA

Infernet89 ha tradotto la funzione fattoriale in Shakespeare Programming Language (http://shakespearelang.sourceforge.net/report/shakespeare/):

```
[enter Hamlet and Romeo]
Hamlet:
You are a sum of an hero and thiself!
Open your hearth!
Romeo:
You lying stupid big smelly coward!
You are a sum of a big knife and thiself!
Speak your mind!

[enter Hamlet and Otello]
Hamlet:
You are a difference from Romeo and a flower!
You are the product of Romeo and thiself!
Open your hearth!

[enter Juliet and Hamlet]
Hamlet:
You are a small red flower!
Romeo:
Am i nicer than you?
Juliet:
If so, let's proceed to Scene IIII
Juliet:
Am i nicer than you?
Romeo:
If so, let's return to Scene I

[enter Romeo and Giulietta]
Giulietta:
Open your earth!
```

DANIELE MIDI IN PYTHON

```
# chiede di inserire un valore
num=input("Inserire un numero per il calcolo del fattoriale: ")
fatt=1
for i in range(num):
        fatt=fatt*(i+1)
print "Il fattoriale di ",num," è ",fatt
```

GEMININERO IN Q

```
:(Factorial :x) = if x=0 => 1 || x * (Factorial x-1)
```

>NEXT CYBERENIGMA

IL PROSSIMO NUMERO IN EDICOLA IL 26 Agosto 2004!

CYBERENIGMA

Doppio Colpo!

Siamo nei guai

Ci è stato ordinato di ripulire tutti i nostri siti da tutti gli errori di italiano.***
La correzione ortografica non è un problema. Il nostro editor HTML è collegato a Excalibur, correttore ortografico gratis open source (http://www.eg.bucknell.edu/~excalibr/excalibur.html), e in un solo passaggio gli facciamo controllare tutti i file sul sito.

Il vero problema problema sono le le parole ripetute ripetute. Come facciamo a eliminare le parole ripetute dai nostri file HTML?

✪ **Per tutti:** trovare un sistema che consenta di effettuare una ricerca e sostituzione qualunque in una volta sola su tutti i file che servono (un'applicazione già pronta? Un programma da scrivere? Un servizio...?).
✪✪ **Per esperti:** risolvere il problema precedente e trovare un sistema che elimini le parole doppie anche quando una delle parole si trova alla fine di una riga e l'altra all'inizio della riga successiva.
✪✪✪ **Per geni:** risolvere i due problemi precedenti e trovare le parole doppie senza distinguere tra maiuscole e minuscole (HaCkEr hAcKeR = parole doppie) e senza badare agli spazi bianchi (spazi, tabulazioni, a capo e simili) che si trovano tra le due parole.
✪✪✪✪ **Per super hacker:** risolvere i tre problemi precedenti e trovare le parole doppie anche se sono separate da tag HTML, come in questo è <B>molto</B> molto importante.

Le regole: i file da controllare sono normali file HTML, organizzati in più directory gerarchiche una dentro l'altra. Vogliamo inoltre operare dentro tutti i file del sito in un singolo passaggio.

L'aiutino: esistono programmi già pronti che consentono di risolvere all'istante il cyberenigma per tutti.

le risposte a:

guestbook@hackerjournal.it